

Best Available Copy

SECURE SYSTEM FOR ACTIVATING PERSONAL COMPUTER SOFTWARE AT REMOTE LOCATIONS

Patent number: JP6501120T

Publication date: 1994-01-27

Inventor:

Applicant:

Classification:

- **international:** G06F13/00; G06F15/00; H04L9/00; H04L9/00;
H04L9/10; H04L9/12

- **european:** G06F1/00N7R2; G06F9/445; G06F9/445N;
G06F21/00N7P5M

Application number: JP19910501845T-19911106

Priority number(s): US19900610037 19901107; US19910682456 19910409

Also published as:

WO9209160 (A1)
EP0556305 (A1)
US5222134 (A1)
EP0556305 (A4)
EP0556305 (B1)

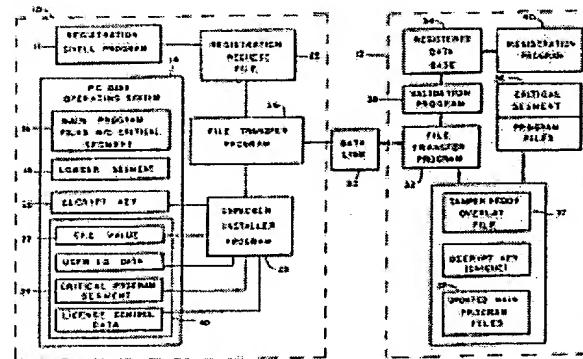
[more >>](#)

[Report a data error here](#)

Abstract not available for JP6501120T

Abstract of corresponding document: US5222134

A process and system for activating various programs are provided in a personal computer. The computer is initially provided with a registration shell. A data link is established between the personal computer and a registration computer. By providing the registration computer with various information, a potential licensee can register to utilize the program. Once the registration process is complete, a tamperproof overlay program is constructed at the registration computer and transferred to the personal computer. The tamperproof overlay includes critical portions of the main program, without which the main program would not operate and also contains licensee identification and license control data.



Data supplied from the esp@cenet database - Worldwide

(19)日本国特許庁 (JP)

(12) 公表特許公報 (A)

(11)特許出願公表番号

特表平6-501120

第6部門第3区分

(43)公表日 平成6年(1994)2月3日

(51)Int.Cl.¹ 認別記号 序内整理番号 F I
 G 06 F 13/00 3 5 1 H 7368-5B
 15/00 3 3 0 A 7459-5L
 H 04 L 9/00
 9/10

7117-5K H 04 L 9/00 Z

審査請求 有 予備審査請求 有 (全 8 頁) 最終頁に続く

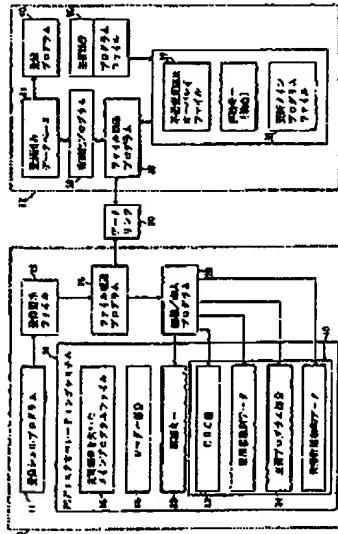
(21)出願番号 特願平4-501845
 (86) (22)出願日 平成3年(1991)11月6日
 (85)翻訳文提出日 平成5年(1993)5月7日
 (86)国際出願番号 PCT/US91/08069
 (87)国際公開番号 WO92/09160
 (87)国際公開日 平成4年(1992)5月29日
 (31)優先権主張番号 610,037
 (32)優先日 1990年11月7日
 (33)優先権主張国 米国(US)
 (31)優先権主張番号 682,456
 (32)優先日 1991年4月9日
 (33)優先権主張国 米国(US)

(71)出願人 タウ・システム・コーポレイション
 アメリカ合衆国 バージニア州 フォルス
 チャーチ、リースバーグ バイク、
 7115、スース327
 (72)発明者 ワイト、デービット、ピー
 アメリカ合衆国 バージニア州 22032、
 フェアファックス ギルバートソン ロー
 ド、4220
 (72)発明者 リッセル、ホレイス、ジー
 アメリカ合衆国 バージニア州 22021、
 チャンチリイ、パレイ カウントリ ドラ
 イブ、13811
 (74)代理人 弁護士 倉持 晴 (外1名)
 最終頁に続く

(54)【発明の名称】 パーソナルコンピュータのソフトウェアを遠隔位置で起動するための安全システム

(57)【要約】

様々なプログラムを起動するための過程とシステムがパーソナルコンピュータ(10)に提供されている。パーソナルコンピュータ(10)には、登録シェルプログラム(11)が当初備わっている。データクリンク(30)がパーソナルコンピュータ(10)と登録用コンピュータ(12)の間に確立される。登録用コンピュータ(12)に様々な情報を与えることにより、見込み被許諾者はメインプログラム(16)の使用を登録することができる。ひとたび登録過程が完了すると、不正変更防止オーバーレイプログラムが登録用コンピュータ(12)において作成され、パーソナルコンピュータ(10)に転送される。不正変更防止オーバーレイには、メインプログラム(16)の主要部分がふくまれ、これを欠くとメインプログラム(16)は動作せず、また不正変更防止オーバーレイには使用許諾監視データと使用許諾制御データも含まれている。



Best Available Copy

〔請求の範囲〕

1. アップロードファイルを複数する方法であつて、
 - 該装置を有する端末コンピュータに対して、ローダーセグメントと登録シェル部分を含むプログラムファイルを提供し、上記プログラムファイルは起動部を欠いてい、上記プログラムファイルを正しく実行することを防止する工程、
 - 使用者識別情報を上記登録シェル部分に入力する工程、
 - 上記使用者識別情報を、上記登録シェルから登録用コンピュータ内にある設立した登録プログラムに送り、上記登録プログラムは使用者識別データと上記登録部分とを併せて各自のオーバーレイファイルを作成する工程、
 - 上記各自のオーバーレイファイルを上記登録プログラムから上記登録シェルに伝達する工程、上記オーバーレイファイルには上記プログラムファイルには当初欠けている主要部分が含まれ、そして
 - 上記オーバーレイファイルを上記メインプログラムファイルに導入する工程を有し、上記オーバーレイファイルに入っている使用者識別が導入されたときだけ上記プログラムファイルの動作が可能とすることを特徴とする請求のプログラムファイル起動方法。

2. 上記オーバーレイファイルを上記登録用コンピュータから上記遠隔コンピュータに伝達する前に、上記使用者識別情報を利用可能とする工程を有する請求の範囲第1項に記載の方法。

3. 不正変更防止のオーバーレイファイルを作成する工程を有する請求の範囲第1項に記載の方法。

4. 上記不正変更防止オーバーレイファイルが上記オーバーレイファイルを暗号化することによつて作成され、通常元本検査法が上記主要プログラム部分が欠けているプログラムファイルが当該馬ねついていて、このプログラムファイルが動作することを防止し、上記オーバーレイデータ部分は最初のオーバーレイファイルが現在導入されているときだけこのプログラムファイルを起動することができ、上記遠隔コンピュータには登録シェルプログラムが備えられ、上記登録シェルプログラムは使用者が僅々に使用者識別情報を入力することを可能にするような少なくとも一回の遠隔コンピュータと、

 - 登録プログラムと、上記使用者識別情報を送信し処理するための手段と、上記プログラムファイルに欠けている上記主要プログラム部分と使用者識別情報を全部あるいは一部を含む各自のオーバーレイファイルを作成するための手段と、上記オーバーレイファイルを上記遠隔コンピュータに伝達する手段とを備えた登録用コンピュータを有し、
 - 上記オーバーレイファイルを上記遠隔コンピュータに伝達することで、上記オーバーレイファイルに入っている使用者識別が現在導入されているときだけ上記プログラムファイルの動作が可能になることを特徴とする上記プログラムファイル起動システム。

5. 上記遠隔コンピュータと上記登録用コンピュータとの間を結合する電子データリンクと、上記登録用コンピュータと上記遠隔コンピュータの両方に備えられているファイル既存処理を含むことを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

6. 上記オーバーレイが実行のためにロードされるたびに巡回冗長検査法が計算され、上記不正変更防止オーバーレイファイル内に伝送された巡回冗長検査値と比較され、上記オーバーレイファイルが改ざん後変更されているかどうかを判断することを特徴とする請求の範囲第1項に記載の方法。

7. 上記使用者識別情報と上記オーバーレイファイルとが、電子データリンクを介して上記登録シェルと上記登録プログラムとの間を伝達されることを特徴とする請求の範囲第1項に記載の方法。

8. 上記登録シェルプログラムが、上記の設立した登録用コンピュータを備えた第二の遠隔コンピュータから離れた、第一のコンピュータ内に残されていることを特徴とする請求の範囲第1項に記載の方法。

9. 上記使用者識別と上記オーバーレイファイルが、一方のコンピュータに入力され読み込まれることを特徴とする請求の範囲第1項に記載の方法。

10. プログラムファイルを削除されながらもしくは削除されない期間を監視するためのシステムにおいて、

 - オーバーレイローダー部分が含まれているが少なくとも一つの

11. オーバーレイファイルを作成するための上記手段が、巡回冗長検査法を備える不正変更防止オーバーレイファイルを作成するための専用装置と記述キーを備えており、上記装置キーは上記オーバーレイファイルと共に上記遠隔コンピュータに伝達されることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

12. 上記遠隔コンピュータが、上記オーバーレイファイルを解説し、上記オーバーレイファイルが実行のためにロードされるたびに巡回冗長検査を計算し、そしてこの検査値を上記登録用コンピュータによって上記オーバーレイファイルと共に伝送された巡回冗長検査値と比較するための手段を備えていることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

13. 上記主要プログラム部分がエグゼクティブ部御アコグテムであり、そして上記使用者識別情報が使用許諾契約情報であることを特徴とする請求の範囲第10項に記載のアコグテムファイル起動システム。

14. 上記登録用コンピュータが、上記オーバーレイファイルを解説し、上記オーバーレイファイルが実行のためにロードされるたびに巡回冗長検査を計算し、そしてこの検査値を上記登録用コンピュータによって上記オーバーレイファイルと共に伝送された巡回冗長検査値と比較するための手段を備えていることを特徴とする請求の範囲第10項に記載のプログラムファイル起動システム。

15. 上記主要部分がエグゼクティブ部御部分であり、そして上記使用者識別情報が使用許諾契約情報であることを特徴とする請求の範囲第1項に記載の方法。

16. 上記主要プログラム部分がエグゼクティブ部御アコグテムであり、そして上記使用者識別情報が使用許諾契約情報であることを特徴とする請求の範囲第10項に記載のアコグテムファイル起動システム。

17. 上記主要エグゼクティブ部御プログラム部分がプログラムファイル全体を有することを特徴とする請求の範囲第16項に記載のプログラムファイル起動システム。

18. プログラムファイルの使用を制御する方法において、

 - 該装置を有するコンピュータに対してセーダー部分と登録シェル部分を含むプログラムファイルを提供し、上記プログラムフ

特表平6-501120 (9)

ファイルは第一レベルの制御情報を有するエグゼクティブ制御プログラムを有しております。

情報を上記登録シエル部分に入力し、

上記使用許諾契約情報を上記登録シエルから独立登録プログラムに転送し、上記登録プログラムに使用許諾契約データを第二レベルの制御情報を有するエグゼクティブ制御プログラムに付与して独自のオーバーレイファイルを発生し、

上記登録のオーバーレイファイルを上記登録プログラムから上記登録シエルに伝送し、上記オーバーレイファイルには上記第二レベルのエグゼクティブ制御プログラムが含まれております。そして

上記登録オーバーレイファイルを上記主要プログラムファイルに導入し、上記プログラムファイルの第二レベルの操作の動作が上記オーバーレイファイル内の使用許諾契約情報が現在導入されているものだけ可能になることを特徴とする上記のプログラムファイル使用の制御方法。

19. 上記オーバーレイファイルを上記登録専用コンピュータから上述機器に伝送する場合に、上記使用許諾契約情報を有効化する工程を有する請求の範囲第18項に記載の方法。

20. 不正変更防止にならっているオーバーレイファイルを作成する工程を有する請求の範囲第18項に記載の方法。

21. 上記不正変更防止オーバーレイファイルが上記不正変更防止オーバーレイファイルを暗号化キーで暗号化することにより作成され、巡回冗長検査を上記暗号化不正変更防止オーバーレイファイル内に提供するとともに解説キーを上記不正変更防止オーバーレイファイルに提供し、上記暗号化および解説キーは上記オーバーレイファイルの独自の内容によって独自に決定されることを特徴とする請求の範囲第20項に記載の方法。

上記登録シエルプログラムは使用者が様々な使用許諾契約情報を入力することを可能にするよう少なくとも一回の差隔コンピュータと、

登録プログラムと、上記使用許諾契約情報を受信し処理するための手段と、第二レベルの機能を有するプログラムモジュールと使用許諾契約情報の企画あるいは一部を含む独自のオーバーレイファイルを作成するための手段と、上記オーバーレイファイルを上記登録コンピュータに伝送する手段とを備えた登録用コンピュータとを有し、

上記オーバーレイファイルを上記登録コンピュータに伝送することで、上記オーバーレイファイルに入っている使用許諾契約情報が実在傳わっているときだけ、上記プログラムファイルの第二レベルの操作動作が可能なることを特徴とする上記システム。

22. 上記登録コンピュータと上記登録専用コンピュータとの間に電子データリンクを有し、ファイル転送装置が上記登録用コンピュータと上記登録コンピュータの両方に組みられていることを特徴とする請求の範囲第27項に記載のシステム。

23. 上記登録用コンピュータが、すべての登録済み登録者が含まれる中央データベースと上記使用許諾契約情報を有効化する手段とを備えていることを特徴とする請求の範囲第27項に記載のシステム。

30. オーバーレイファイルを作成するための上記手段が、巡回冗長検査が記述されている不正変更防止オーバーレイファイル作成するための暗号化キーと解説キーとを備えており、上記解説キーは上記オーバーレイファイルと共に上記登録コンピュータには送り、上記暗号化および解説キーはファイルの内容によって独自に決定されることを特徴とする請求の範囲第27項に記載のシステム。

22. 新しい巡回冗長検査値が、上記オーバーレイが実行のためにロードされるたびに計算されて、上記オーバーレイファイルと共に保存された巡回冗長検査値と比較され、上記オーバーレイファイルが作成時は変更されているかどうかを判断することを特徴とする請求の範囲第21項に記載の方法。

23. 上記登録用コンピュータと上記オーバーレイファイルが、上記登録シエルと上記登録プログラムとの間を電子データリンクを介して伝送されることを特徴とした請求の範囲第18項に記載の方法。

24. 上記登録シエルプログラムが、上記独立登録プログラムを備えた第二のコンピュータから離れている第一のコンピュータに得えられることを特徴とする請求の範囲第16項に記載の方法。

25. 上記有効化により上記使用許諾契約情報を正式の登録シエルを全ても保することを特徴とする請求の範囲第19項に記載の方法。

26. 上記使用許諾契約情報を上記オーバーレイファイルが一台のコンピュータに人力され、読み取ることを特徴とする請求の範囲第18項に記載の方法。

27. 制限されたあるいは削除されない期間、プログラムファイルをアップグレードするシステムにおいて、

第一レベルの機能を有するプログラムを含むオーバーレイローダー部分を含むプログラムファイルが書き換わって、上記オーバーレイローダー部分は本体のオーバーレイファイルが現在導入されているときだけこのプログラムファイルを起動することができ、上記遠隔コンピュータには登録シエルプログラムが備えられ、

テム。

31. 上記遠隔コンピュータが、上記オーバーレイファイルを解説し、上記オーバーレイファイルが実行のためのロードされるたびに新しい巡回冗長検査値を計算し、そしてこの検査値を上記登録用コンピュータにより上記オーバーレイファイルと共に伝送された巡回冗長検査と比較するための手段を備えていることを特徴とする請求の範囲第30項に記載のシステム。

【 申 請 書 】

パーソナルコンピューターのソフトウェアを遠隔位置で起動するための安全システム

背景の説明

一般的に、パーソナルコンピューターあるいはそれに類似した装置の使用者の大半は、それら装置で実行するソフトウェアを様々な小売店からあるいは複数販売元を通じて入手する。いずれの場合も、ソフトウェア製品はいわゆる「紙面包装」材で包装されており、その収納用封筒を破った時点でのソフトウェア製品に対する使用許可契約が成立し、その製品の使用許可権を該使用許可者／購入者による承認可視契約あるいは使用から保護するようになっている。この方法による通行時は、許諾者と被許諾者の双方にとって満足すべきものではないことが分かっている。たとえば、被許諾者にとっては、ソフトウェアプログラムを動作させてみてからそれが被許諾者が必要としているものかどうかを判断する場合が多々ある。さらに、許諾者の間からみると、この方法では被許諾者の識別ができないうえ、許諾者によるプログラム使用の制御あるいは監視を行なうことができない。

ソフトウェアブリゲード方式は、Thomasの米国特許第4,740,830号は、本発明の米国特許第4,446,519号に複数開示されており、プログラム開発された「はい／いいえ」で答える機能がプログラムに組み込まれており、そのソフトウェアが使用許可されるコンピュータに配置されているパーソナルコンピューターあるいはファームウェア保護装置の存在を確認するようになっている。この技術の不足は、プログラムが修理的保護装置をしでは使用できないようにすることであり、これはソフトウェアよりも復元することができるに因る。しかし、このような技術は、正しい代理店等が見抜かれ、そしてそれをわずかに変更してプログラムに書き込まれてしまえば、簡単に打ち祓られてしまう。ひとたび打ち祓われると、無効化の遠隔コピーが生成され記録される可能性がある。

本発明の方針とシステムに関する。動作可視プログラムは、購入者／被許諾者と版元者／許諾者との間の特定の契約において入手可能となる。版元者と購入者との関係は、本発明の目的に關しては、許諾者／被許諾者契約の関係である必要はないが、以下では版元者を版元者、購入者を被許諾者としくは使用者と呼ぶ。ひとたび被許諾者が特定の契約条件に合意すると、被許諾者識別データが登録用コンピュータに与えられる。登録用コンピュータはその費用を免除し、使用許可されたプログラムの可視部分を提供する。これらの操作は不正見抜止が施されていると同時に、誤認された被許諾者にとって被のものとなっている。この情報の交換に基づき、版元コンピュータプログラムが登録用被許諾者のコンピュータに不正見抜止をファイルに吸納して反映される。同時に、このファイルには使用者独自の情報を含めている。本発明の実施例としては様々なるが考えられるが、いずれの実施例も被許諾者を識別する独自のデータと保護されているソフトウェアプログラムに関する情報とが含まれている。暗号化バッケージの構成を示している。したがって、被許諾者は版元ではなく、そして保護されたソフトウェアは使用許可契約に違反できる情報を守り化される。さらに、使用許可開拓データを暗号化バッケージに含めることにより、使い方を制限して使用許可契約の条件を遵守させることができる。

一般的に、様々な実施例は、ソフトウェアのデモンストレーション版を有する可能性のあるマーケティングシェルプログラムの最初の構造が使う。このシェルプログラムは、見本表示と首次記述だけを有しているか、あるいは完全なプログラムの動作不能版を有している。しかし、大部分の実施例は、登録プログラムと、ローダーセグメントと呼ばれる特別のプログラムモジュールを含むよう構成になっている。

マーケティングシェルは選択な方法で自由に配布されるであろう。マーケティングシェルがプログラムのデモンストレーション

特表平6-501120 (4)

Filfileの米国特許第4,740,830号は、中央（遠隔）コンピュータを使用して、正しい符号の入手を試みる悪意のプログラマがアクセスできないマスクリストあるいはアルゴリズムから弄られたコット削除コードあるいは有効化コードを提供することを示している。しかし、この方法は、仮想オフコードを收受することにより、あるいは見抜の周囲をプログラミングすることにより、もしくはデバッグプログラムによりプログラムを分析してプログラムの実行を可能にするコードの存在を見つけ出すことにより、簡単に見抜られてしまう。ひとたびこの保護が打ち祓われると、動作可能なプログラムの無効版のコピーが叩き書きされる可能性がある。

さちに、Schildの米国特許第4,849,510号に示すされている方法では、最も価値のあるアルゴリズムを無効化し、無効化されたプログラムを実験装置内で実行すると同時に、回復アルゴリズムを別の物理的に分離し保護された処理装置で実行することにより回復し、有効装置を2つの処理間の相互作用によって獲得するようになっている。このような技術は、回復アルゴリズムの物理的保護に依存しており、この技術的保護が侵害された場合、本発明のプログラムによって簡単に打ち祓われる可能性がある。したがって、そのような方法は、複数機器の物理的保護が無効できない大変さを有においては、実用的ではない。

そのため、ソフトウェアを使用許可生産から保護しつつソフトウェアを大量市場に配布するための技術を公表が求められる。さらに、見るみ購入者／被許諾者がソフトウェア製品を購入前に試してみることができような方法とシステムの要である。また、ソフトウェア製品の改良および更新部分を登録使用者に配布するための方法も必要である。

説明の概要と範囲

本発明は、パーソナルコンピューターのソフトウェアプログラムあるいは他の種類のプログラムを、使用許可を管理した方法で配

版を有している場合、エグゼクティブ複数ループが保護されたプログラムの歴史版になる。マーケティングシェルは組み込み使用者に登録する。マーケティングシェル内の登録プログラムは、登録データを登録データベースコンピュータに送信する。暗号化ファイル内で結合された被許諾使用者独自のデータと動作可視版のプログラムとを有する独自の符号化パッケージが組み立てられる。独自の符号化キーが、暗号化ファイルおよび保護されていないプログラムファイルと共に使用者のコンピュータに伝送されるが、これらはマーケットシェルを最大化する。誤認キー、暗号化ファイル、そして保護されていないファイルの剥離と同時に、マーケットシェルはこれらの各々を使用者のコンピュータに導入する。

したがって、使用者がプログラムを実行する毎に、ロードセグメントが提供された暗号キーを使用して、暗号化ファイルを保護されていないファイルに対するオーバーレイとしてロードして解説する。このプログラムは保護されていないソフトウェアプログラムの設計にしたがって実行され、独自の使用許可データもプログラム実行中にロードされる。プログラムが実行されていないときは、保護されているマニフェストはその暗号化版に留まって、保護されていないプログラムファイルと共にコンピュータの大容量記憶装置に組み込まれている。保護されているプログラムは実行のためにロードされたときだけ解説され、正しい暗号化キーにアクセスしなければ実行され得ない。

図面の概要と範囲

図1は本発明による登録履歴を示す流れ図である。

図2は本発明によるプログラム実行過程を示す流れ図である。

図3は、本発明の実施による代表的なパーソナルコンピュータと登録用コンピュータの接続図である。

図4は、本発明の知見によると代表的なパーソナルコンピュータと登録用コンピュータに代る実施例を示す接続図である。

登録の詳細を説明

本発明の目的は、許諾者がそのプロセラムの費用対効果に関する貴重情報を従来使用されている方法よりはるかに効率的な方法で維持することを可能にすることである。さらに、本発明の第二の目的は、被許諾者あるいは使用者が特定のプログラムの購入あるいは使用許諾を得る前に実行することを可能にすることである。さらに、本発明の更なる目的は、特定のプログラムの使用許諾権がされたアップグレード権を登録被許諾者に配布する手段を提供することである。したがって、本発明の知見は包括的なものと考えられ、そしてどのようなソフトウェアプログラムも本方法によって配布できるものと想定されている。

一実施例において、動作可能なエグゼクティブプロセラムを取いで完全な製品アドリブが、パーソナルコンピュータあるいは他の装置において、aceutディスク、ファームウェア、ハードウェアあるいは他の手段で最初に提供される。さらに、この特定アドリブには登録シェルプログラムも含まれる。ただし、小さいアドリブもしくは複数の異なるアドリブがある場合、プログラム自体は存在せず、シェルだけが提供される。ニザゲクティア制御ループが除外されているため、このプログラムは正しい登録過程を実現しなければ動作しない。図1および図2に示されているように、この登録過程は、パーソナルコンピューター(PC)の内部の登録シェルプログラム11と登録用コンピューター12内部に格納されている登録プログラム40とを使用して開始される。登録システムプログラムが登録用コンピューター12内に格納され、電子データリンク30を介して登録シェルプログラムがアクセスできる。この電子データリンクは、ローカルエリアネットワークでもよく、電話 modemリンクでもよく、あるいはその他のいかなる接続であってもよい。ただし、第二の実施例においては、登録シェルおよび登録システムプログラムは同一の媒体上に存在してもよいが、その媒体は製品専用プログラムとは別でなければならない。この場

特表平6-501120(5)

合、登録シェルおよび登録システムプログラムが入っている専用可能な媒体は、許諾された導入プログラムによって使用者パーソナルコンピューター10へ機器的に移植され、電子データリンクは必要ではない。

登録シェルプロダクツは、使用者がPCオペレーティングシステム14のメインプロダクツファイル内に提供されている製品専用プログラムの実行を最初に実行すると実行される。登録シェルは、製品専用プログラムに関する起動情報を提供しそれをPC表示装置に表示すると同時に、見込み被許諾者を促して登録者として登録する。使用者登録は、特定の使用場所における特定の被許諾者に対して施設され、その周囲は幾々な量をもしくは一時的でよく、そのための費用は被許諾者に対して課せられない。ただし、登録シェルは、不正変更防止オーバーレイファイルが存在しないかどうか、メインプログラムを実行しない。登録シェルプログラム11は、被許諾者のPCに表示されるアカウント形式を提供し、被許諾者に対して、請求書送付先、ロードキー、使用許諾条件などの識別情報を提供をする。この情報は、被許諾者が再確認する登録箇所ファイル25に入力される。そして、登録シェルプログラムは、被許諾者の指定キーを押して登録を開始するのを待つ。このキーが押されると、登録ファイルが固く、そして登録シェルファイル伝送プログラム26が登録システムファイル伝送プログラムとのデータリンクを確立する。登録用コンピューター内の登録プログラム40は、データリンクが正確な登録シェルで確定されていることを確認する検査保護チェックを実行する者活性手段42によって保護される。つぎに、登録シェルは登録要求ファイル35を、そのファイルを受信する登録システムに転送し、必要な二ラーチェックと、結合されたファイル伝送プログラム26および52間のヘンドショータ動作を実行する。完全な登録要求ファイルが中央登録用コンピューターで実現されたると、登録要求が登録済み使用者34のデータベースに記して確認される。確認には、その裏面に答えるべきかど

うかを判断する様々なチャックが含まれる。たとえば、一時的使用専用に対する要求が特定の被許諾者から再度送られてきた場合、その被許諾者には使用許可が与えられず、そしてそのプログラムのニザゲクティア制御ループは退出されない。そのような状態が発生した場合、通常のメッセージが登録システムに伝送され、見込み被許諾者に対して表示される。しかし、要求が確定されると、登録済み使用者データベースへの記録が作成されるが、この過程全体が完了するまで、そのデータベースには入力されない。

登録用コンピューター12の内部では、つぎに使用登録アーケが使用されて、登録用新データとエグゼクティブ制御ループアドリブを合30とを結合することにより作成された独自の不正変更防止オーバーレイファイルが生成される。結合されたデータとアドリブファイルに各自で、不正変更防止オーバーレイファイル内に含まれる無研究登録(CRC)値が計算される。一式の独自の暗号化キーと暗号キーが作成され、不正変更防止オーバーレイファイルの内容全体が暗号化キーを使用して暗号化される。この暗号化キーに基づき、不正変更防止オーバーレイファイルと共に暗号化される暗号キーが提供される。暗号化アルゴリズムは、暗号化システムのように、暗号化と解密がそれぞれ異なるキーを使用する状態ではならない。登録システムが、不正変更防止オーバーレイファイルと解密キーを、パーソナルコンピュータ登録シェルに伝送される1個の出荷ファイル38に組み込む。また、更新されたメインプログラムファイルもこの出荷ファイルに組み込まれ、ファイル伝送プログラムとともに独立してあるデータリンクとを組じてPCの登録システムに伝送される。

出荷ファイル一式の登録と同時に、登録シェルプログラム内の開拓へ導入プログラムは化而ファイルを開き、エグゼクティア制御ループセグメント24、CRC注22をもじりに解説マー20および、含まれている場合は、更新メインプログラムファイルを含む不正変更防止オーバーレイファイル40を導入する。これで登録過程が

完了したので、電子データリンクを切断する。登録データベースレコードが入力され、そして被許諾者の要求に対する結果が、中央登録用コンピューター12における別のプログラムによって実行される。

登録が終了すると、被許諾者のパーソナルコンピューターに導入された登録済み製品専用プログラムを起動して、不正変更防止オーバーレイファイルと解密キーを使用して製品専用プログラムを実行するたびに実行する製品専用プログラムをロードするためのプロセスが開始される。

このプログラム実行過程を図1に示す。図示されているように、パーソナルコンピューターの使用者が製品専用プログラムの実行をオーバーレイデングシステムに命じると、オペレーティングシステムはメインプログラムとローダーセグメントをロードする。ローダーセグメントは他のすべてのプログラムを命じて実行される。つぎに、ローダーセグメントは製品専用プログラムの起動を実行し、不正変更防止オーバーレイの存在をチェックする。不正変更防止オーバーレイが導入されていなければ、ローダーセグメントは終了してオーバーレイデングシステムに戻るので、メインプログラムファイルの実行が事前に防止される。不正変更防止オーバーレイが導入されていれば、ローダーセグメントは解密キーを見つけて不正変更防止オーバーレイの解読とロードを行ない、メインプログラムファイルに対して存在しないエグゼクティア制御ループプログラムを命じならびに独自の操作および使用許諾制御アーケを起動させる。解読およびロード過程において巡回冗長性検査が実行され、それが完了すると、不正変更防止オーバーレイが登録用コンピューターからパーソナルコンピューターに伝送されたときに作成された不正変更防止オーバーレイに記憶された巡回冗長性値と比較される。巡回冗長性が失敗に終わると、そのオーバーレイは最初の方針によって復元が與えられたものとなる。したがって無効とされる。この時点で、ローダーセグメ

ントはそのオーバーレイを取り外し、終了してオペレーティングシステムに戻る。したがって、不正変更防止オーバーレイが含まれていない場合と同様に、メインプログラムファイルの実行は、不正変更防止オーバーレイとの部分が変更されていても、事前に防ぐされる。専用冗長検査の結果、オーバーレイが変更されていないことが確認されると、ニーサセグメントはオーバーレイを含めたメインプログラムファイルの実行を開始し、そして製品専用プログラムが最後まで実行される。

不正変更防止オーバーレイを動作可能形態の製品専用プログラムに含めることを要求することにより、専用冗長検査と使用許諾制御データはそれ以前動作可能プログラムに常に含まれられることになる。このようにして、許諾者は不正使用を防止するとともに監視することができる。

図1および図2を参照しながら説明したように、本発明によると、登録過程によって、メインプログラムファイルのニグゼタディアブ制御ループセグメントと専用冗長制御データとを含む不正変更防止オーバーレイファイルが生成される。登録過程が完了すると、この不正変更防止オーバーレイは登録専用コンピュータからパーソナルコンピュータに転送される。この不正変更防止オーバーレイは、起動後に不正履歴を防止するキー装置である。なぜなら、エグゼクティブ制御ループプログラムを今は、専用なしには独自の使用許諾制御データと専用冗長制御データから分離することもできなければ、専用冗長制御データと専用冗長制御データも発見なしには変更できないからである。

この不正変更防止オーバーレイファイルは、オーバーレイファイルが生成されるときに最初に巡回冗長検査値をオーバーレイファイルに記憶させるとで不正変更防止になるとみなされる。巡回冗長検査値は、プログラム命令と専用冗長制御データを含むオーバーレイファイルの内部全体に対して計算される。被許諾者データは各自であるので、各々のCRCは取扱なものにする。記述されてい

特表平6-501120(6)

るCRC値が、オーバーレイがロードされるたびにローダーセグメントによって計算された巡回冗長検査値と比較される。これらの巡回冗長検査値が一致しなければ、ローダーセグメントは終了してオペレーティングシステムに戻る。したがって、オーバーレイファイルの内容になんらかの変更が加えられていれば、記述されている巡回冗長検査値に対応する変更が行われない限り、そのオーバーレイファイルは無効となる。つぎに、不正変更防止オーバーレイの内容全体が、巡回冗長検査値の生成が不明になるような方法で暗号化されるので、この種の潜在をつきとめてそれを変更することが困難になる。

また、暗号化により、不正変更防止オーバーレイに含まれる特定のプログラム命令をさらに独自の使用許諾制御データが書きにくくなる。暗号化は、専用冗長検査値システムのように暗号化と解読に別々のキーを使用する複数によって達成される。暗号化ならばに専用の符号化キーと上級符号化キーのためのアルゴリズムは登録システム内に搭載し、したがって専用冗長者にはアクセスが不可能である。解読キーは、登録システムと登録プログラムシェルを通じて被許諾者のコンピュータに伝送される。オーバーレイファイルを解読するためのアルゴリズムはローダーセグメント内にあるので、解読キーと解読アルゴリズムを使用してオーバーレイファイルを解読しその内容を検査することは、因縁ではあるが可能である。しかし、内容を変更して、新しい変更されたオーバーレイファイルを暗号化するほどの、暗号化キーに対するアクセスができないために阻止される。私的暗号化キーで暗号化されたオーバーレイファイルだけしかあ公共暗号解読キーで解読できず、私のキーは公共キーから容易には得られないというのが、公共暗号等システムの一特徴である。

不正変更防止オーバーレイファイルは、プログラム命令のエグゼクティブ制御ループセグメントと、専用冗長の方法と制御に適用可能な専用冗長制御データとを有している。このデータには、

製品専用の制御、コンピュータの製造番号、コンピュータのモデルの製造番号、そしてその他の情報を含まる。

ローダーセグメント18は若狭自動のサブプログラムであり、これは、ローダーアセグメントが取り除かれたり迂回された場合、メインプログラムファイルを動作不能にする仕組によって専用専用プログラムのメインプログラムファイルに替わる。この場合抜取は、特定のプログラム命令と製品専用プログラムのメインプログラムファイル内部に内蔵するプロセスである。これらの内部された命令は、使用者にとっては未知の記憶位置にある専用の位置を検索する。ローダープログラムセグメントを実行すると、既定の値がメインプログラムファイルの動作を可能にするために必要な特定の記憶アドレス位置に記憶される。ローダープログラムセグメントは、その他の操作の間にこの動作を実行する。したがって、ローダーセグメントを取り外したり迂回したりすると、メインプログラムファイルには特定の位置における特定の値が含まれないことになり、そのため動作不能になる。

次の実施例において、登録シェルは、製品専用プログラムの動作可能なデモンストレーション版を含んでいる可能性があるマーケティングパッケージの一例として述べられる。デモンストレーション版のプログラムは、ローダーセグメント、デモンストレーション版の解説キー、そしてデモンストレーション版の不正変更防止オーバーレイを含むように設計されている。この場合、不正変更防止オーバーレイには独自の専用冗長制御データは含まれないが、製品版の製品の機能と表示のデモンストレーションだけを行なうメインプログラムエグゼクティブ制御ループが含まれるであろう。デモンストレーション版のニグゼクティブ制御ループは、エグゼクティブ制御ループの機能設計によって設計されたプログラムの通りを操作を有している。たとえば、選択肢を提供するデモンストレーションメニューをプログラムとして選択肢を表示することができるが、デモンストレーション版のエグゼクティブ

制御ループをプログラミングして選択項目を製品登録情報として表示して、製品を動作させる前に登録することを意味である。

登録を開始する前に、見込み登録者はプログラムを実行し、デモンストレーション版が実行されであろう。前述したとおりに示したように、デモンストレーション版の解説キーが使用され、デモンストレーション版のエグゼクティブ制御ループがロード、実現、そして実行される。デモンストレーション版が終了すると、見込み登録者は、専用化として登録登録版のプログラムを保存するための一時的使用許諾を得るように指示される。そして、使用者は前述のようにして登録を行い、図4に示されているプロセスを開始することができる。登録要求にて新規として、新しいオーバーレイファイル40'を専用の解説キー20'が含まれている専用ファイルが登録用コンピュータから送られる。追加プログラムファイルと専用版のプログラムファイルも、専用ファイルと共に受信される。登録プログラムはデモンストレーション版の不正変更防止オーバーレイ40と解説キー20をそれぞれの登録版40'と20'で置換する。

登録後も、使用者がプログラムを実行すると、プログラム実行過程で専用読み版の不正変更防止オーバーレイ40'が検出されてロードされ、専用の解説キー20'を使用することにより、専用読み版のエグゼクティブ制御ループが呼び出され実行される。このようにして、デモンストレーション版は完全に動作する登録版に変換される。

プログラムの実行向上版が利用できる場合、使用者は同一のプロセスを実行してさきに別の解説キーと、より強化されたニグゼクティブ制御ループと追加プログラムファイルを有する別の不正変更防止オーバーレイとを受信して、より強化された版の製品に更新することができます。

様々な実施例が、小さな不正変更防止オーバーレイを使用して大きなプログラムの制御を行なうための違う典型的な方法を使

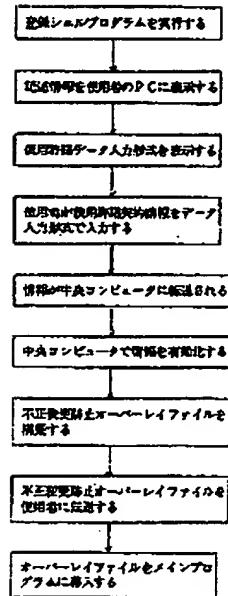
用することができる。このような状況は、ここにも含まれている
ように、プログラムの部分あるいはプログラム全体を使能解説表
と結合する形式で記述するため、ここに開示されている方法
がもたらす両面的利點の可能性の單なる例である。

上記の知見に照らし合わせ、本発明は様々な登録形態が可能なこととは明らかである。たとえば、本発明では、使用者のコンピュータがその地域の登録用コンピュータに接続され、さらにはその登録用コンピュータがそれより広い地域の登録用コンピュータに接続され、というように階層構造的に実現することも可能である。その他の登録用コンピュータの登録構造は、その地域の登録用コンピュータをそれより広い地域の登録用コンピュータとの契約に含まれる登録料金割引率によって制御できるであろう。したがって、下記の各登録方式の範囲内であれば、本発明を上記記載事項に説明されている以外の方法で実施することができる。

招考平6-501120(7)

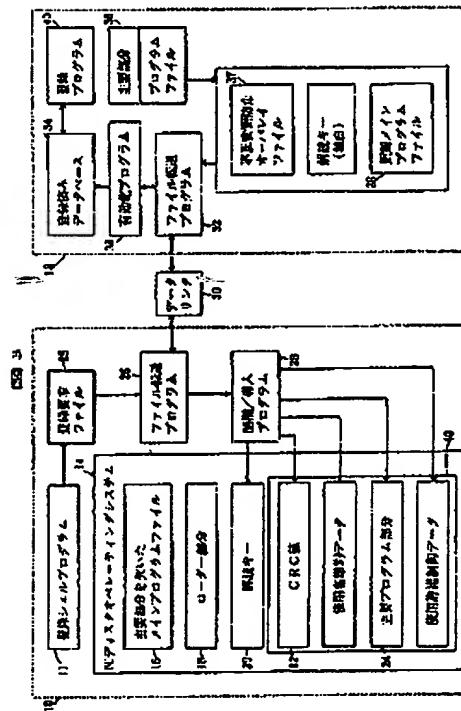
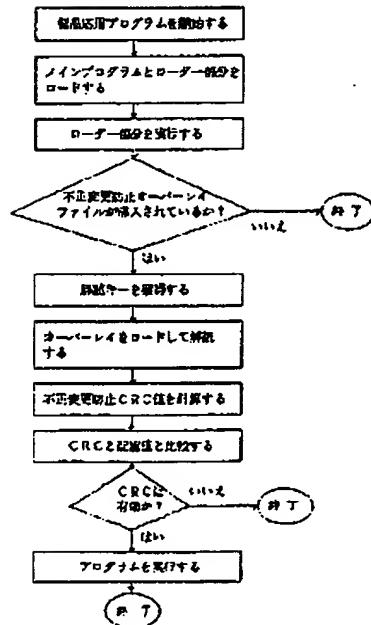
三

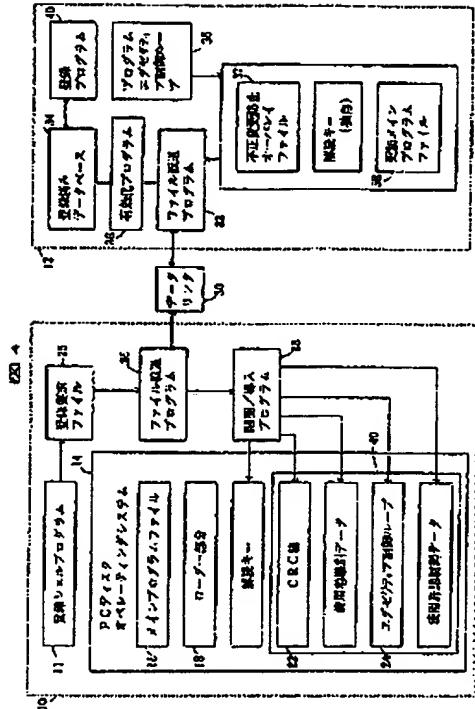
登錄通報



四 2

ブロクラム実行過程





フロントページの読み

(51) Int.Cl.⁵ 分別記号 廣內整理番号 F
H 04 L 9/12

(61) 指定国 EP (AT, BE, CH, DE,
DK, ES, FR, GB, GR, IT, LU, NL, S
E), CA, JP